2009 DRAFTING REQUEST

Bill

Received: **11/13/2008**

Received By: **rnelson2**

Wanted: **As time permits**

Identical to LRB:

For: **Marlin Schneider (608) 266-0215**

By/Representing:

This file may be shown to any legislator: **NO**

Drafter: **phurley**

May Contact:

Addl. Drafters:

Subject: **Courts - evidence**

Extra Copies:

Submit via email: **YES**

Requester's email: **Rep.Schneider@legis.wisconsin.gov**

Carbon copy (CC:) to:

Pre Topic:

No specific pre topic given

Topic:

Admissibility of digitally produced evidence

Instructions:

See attached 07-0686 (AB14) t/c to schneider's office: they want to prevent law enforcement from submitting altered videos/photos. t/c 9-2-09: if I only put "law enforcement,' then otherwise submitting an altered video/photo would be allowed. Is that what they want? Also, if submitting altered video is a misdemeanor, who would be charged? The attorney? The DA, if it's a law enforcement video/photo? Aaron will be out until september 20 - either wait until then or another aide will take a look and get back to me on these questions. t/c to Aaron 9-29: he'll ask about who to charge. Probably need to rework the whole thing so as to target the law enforcement agencies, though, without allowing anyone to submit an altered document if they know it's altered and the alteration is not part of the case.

Drafting History:

Vers.	Drafted	Reviewed	Typed	Proofed	Submitted	Jacketed	Required
/?	rnelson2 11/14/2008			_____ _____			S&L Crime

Vers.	Drafted	Reviewed	Typed	Proofed	Submitted	Jacketed	Required
/1	phurley 11/17/2008	kfollett 12/01/2008	rschluet 12/01/2008	_____ _____	mbarman 12/01/2008	cduerst 02/18/2009	S&L Crime
/2	phurley 10/12/2009	kfollett 10/15/2009	rschluet 10/15/2009	_____ _____	cduerst 10/15/2009	cduerst 10/15/2009	

FE Sent For: attn
/2 12/18/09

<END>

2009 DRAFTING REQUEST

Bill

Received: **11/13/2008**

Received By: **rnelson2**

Wanted: **As time permits**

Identical to LRB:

For: **Marlin Schneider (608) 266-0215**

By/Representing:

This file may be shown to any legislator: **NO**

Drafter: **phurley**

May Contact:

Addl. Drafters:

Subject: **Courts - evidence**

Extra Copies:

Submit via email: **YES**

Requester's email: **Rep.Schneider@legis.wisconsin.gov**

Carbon copy (CC:) to:

Pre Topic:

No specific pre topic given

Topic:

Admissibility of digitally produced evidence

Instructions:

See attached 07-0686 (AB14) t/c to schneider's office: they want to prevent law enforcement from submitting altered videos/photos. t/c 9-2-09: if I only put "law enforcement,' then otherwise submitting an altered video/photo would be allowed. Is that what they want? Also, if submitting altered video is a misdemeanor, who would be charged? The attorney? The DA, if it's a law enforcement video/photo? Aaron will be out until september 20 - either wait until then or another aide will take a look and get back to me on these questions. t/c to Aaron 9-29: he'll ask about who to charge. Probably need to rework the whole thing so as to target the law enforcement agencies, though, without allowing anyone to submit an altered document if they know it's altered and the alteration is not part of the case.

Drafting History:

Vers.	Drafted	Reviewed	Typed	Proofed	Submitted	Jacketed	Required
/?	rnelson2 11/14/2008			_____ _____			S&L Crime

Vers.	Drafted	Reviewed	Typed	Proofed	Submitted	Jacketed	Required
/1	phurley 11/17/2008	kfollett 12/01/2008	rschluet 12/01/2008	_____ _____	mbarman 12/01/2008	cduerst 02/18/2009	S&L Crime
/2	phurley 10/12/2009	kfollett 10/15/2009	rschluet 10/15/2009	_____ _____	cduerst 10/15/2009		

FE Sent For:

<END>

2009 DRAFTING REQUEST

Bill

Received: **11/13/2008**

Received By: **rnelson2**

Wanted: **As time permits**

Identical to LRB:

For: **Marlin Schneider (608) 266-0215**

By/Representing:

This file may be shown to any legislator: **NO**

Drafter: **phurley**

May Contact:

Addl. Drafters:

Subject: **Courts - evidence**

Extra Copies:

Submit via email: **YES**

Requester's email: **Rep.Schneider@legis.wisconsin.gov**

Carbon copy (CC:) to:

Pre Topic:

No specific pre topic given

Topic:

Admissibility of digitally produced evidence

Instructions:

See attached 07-0686 (AB14)

Drafting History:

Vers.	Drafted	Reviewed	Typed	Proofed	Submitted	Jacketed	Required
/?	rnelson2 11/14/2008			_____ _____			S&L Crime
/1	phurley 11/17/2008	kfollett 12/01/2008	rschluet 12/01/2008	_____ _____	mbarman 12/01/2008	cduerst 02/18/2009	

FE Sent For: 12/5 F 10/15 9 12/5 F

<END>

2009 DRAFTING REQUEST

Bill

Received: **11/13/2008**

Received By: **rnelson2**

Wanted: **As time permits**

Identical to LRB:

For: **Marlin Schneider (608) 266-0215**

By/Representing:

This file may be shown to any legislator: **NO**

Drafter: **phurley**

May Contact:

Addl. Drafters:

Subject: **Courts - evidence**

Extra Copies:

Submit via email: **YES**

Requester's email: **Rep.Schneider@legis.wisconsin.gov**

Carbon copy (CC:) to:

Pre Topic:

No specific pre topic given

Topic:

Admissibility of digitally produced evidence

Instructions:

See attached 07-0686 (AB14)

Drafting History:

Vers.	Drafted	Reviewed	Typed	Proofed	Submitted	Jacketed	Required
/?	rnelson2 11/14/2008			_____ _____			S&L Crime
/1	phurley 11/17/2008	kfollett 12/01/2008	rschluet 12/01/2008	_____ _____	mbarman 12/01/2008		

FE Sent For:

<END>

2009 DRAFTING REQUEST

Bill

Received: **11/13/2008**

Received By: **rnelson2**

Wanted: **As time permits**

Identical to LRB:

For: **Marlin Schneider (608) 266-0215**

By/Representing:

This file may be shown to any legislator: **NO**

Drafter: **phurley**

May Contact:

Addl. Drafters:

Subject: **Courts - evidence**

Extra Copies:

Submit via email: **YES**

Requester's email: **Rep.Schneider@legis.wisconsin.gov**

Carbon copy (CC:) to:

Pre Topic:

No specific pre topic given

Topic:

Admissibility of digitally produced evidence

Instructions:

See attached 07-0686 (AB14)

Drafting History:

Vers.	Drafted	Reviewed	Typed	Proofed	Submitted	Jacketed	Required
/?	rnelson2 11/14/2008 phurley	11/17 12/1	12/8	12/8			

FE Sent For:

<END>

Digital watermarking

From Wikipedia, the free encyclopedia

Digital watermarking is the process of embedding information into a digital signal. The signal may be audio, pictures or video, for example. If the signal is copied, then the information is also carried in the copy.

In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this is also a visible watermark.

An image with visible digital watermarking. The text "Brian Kell 2006" can be seen across the center of the image.

In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such. An important application of invisible watermarking is to copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. Steganography is an application of digital watermarking, where two parties communicate a secret message embedded in the digital signal. Annotation of digital photographs with descriptive information is another application of invisible watermarking. While some file formats for digital media can contain additional information called metadata, digital watermarking is distinct in that the data is carried in the signal itself.

The use of the word of watermarking is derived from the much older notion of placing a visible watermark on paper.

Contents

Instance of a Digital Watermarking Scheme

A general watermarking scheme is defined as:

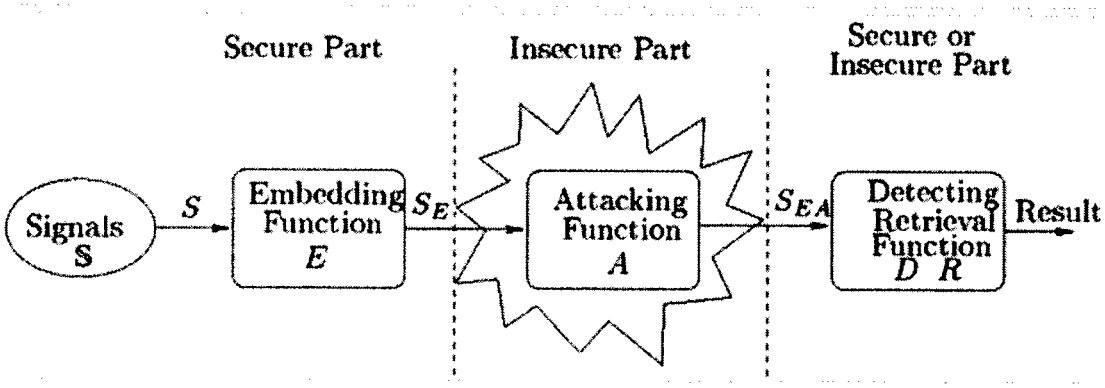
$$\Omega^* = (E, D, R, M, p_E, p_D, p_R)$$

where E defines the embedding function, D detecting function, R retrieval function and M the message. Furthermore, the embedding parameters $p_E \in \mathcal{P}_E$ defines the parameter set used for watermark embedding, $p_D \in \mathcal{P}_D$ defines the detection parameters and $p_R \in \mathcal{P}_R$ retrieval parameters. Hence, each watermarking scheme Ω may have different instances according to the values that these parameters may adopt. An instance Ω^* of the watermarking scheme Ω for a particular value of the parameter vectors.

Watermarking Life-Cycle Phases

In general, the usage of digital watermarking can be simplified as follows. An unmarked (mostly original) signal (S, with $S \in \mathbb{S}$) is the source signal, where the watermark (w) is embedded by using an embedding function E. The result is the marked signal S_E. It can be defined, that this process is done in a secure environment. The following step could be, for example, the distribution of S_E over the Internet or storage of it to provide authenticity or integrity checks. These processes can be seen as an insecure part, where attacks ($A_{i,j} \in \mathbb{A}$) occur on S_E. After distribution of S_E, the signal is defined as S_{EA} because potential attacks could have destroyed the watermark. A detecting function D tries to detect the watermark w or a retrieval function R tries to retrieve the embedded message m'. The detection/retrieval can be done in a secure or insecure environment, depending on the used application of the watermarking algorithm.

The complete scenario is defined as *life cycle* of a watermark, because it begins with embedding and ends with detection/retrieval. This is shown in the following figure with expected secure and insecure parts.



General watermark life-cycle phases with embedding-, attacking- and detection/retrieval functions

The information to be embedded is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal.

The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where pirates attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data, cropping an image or video, or intentionally adding

noise.

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark is still present and it can be extracted. In robust watermarking applications, the extraction algorithm should be able to correctly produce the watermark, even if the modifications were strong. In fragile watermarking, the extraction algorithm should fail if any change is made to the signal.

Watermark Parameters

In general, the fundamental watermarking parameters are classifies into the 7 watermarking properties capacity, complexity, invertibility, transparency, robustness, security and verification (alphabetic order):

Capacity

The Capacity is in general divided into embedding and retrieval capacity.

Embedding Capacity

The embedding capacity cap_E of a watermarking scheme is defined as the amount of information that is (seems to be) embedded into the cover object to obtain the marked object. A simple definition for a capacity measure cap_E would be related to the size of the embedded message, i.e. $\text{cap}_E(\Omega^*, S) = \text{size(M)} = |M|$. In addition, capacity is often given relative to the size of the cover object:

$$\text{cap}_{E\text{rel}}(\Omega^*, S) = \frac{\text{cap}_E}{\text{size}(S)}.$$

Note that such measure only takes into account the information embedded, but not the information that is retrieved. Note, also, that this measure does not consider the possibility of *repeat coding*, in which the mark is replicated as many times as needed prior to its insertion. All these issues are related to the **retrieval capacity** which is defined in the retrieval function.

Retrieval Capacity

The definition of retrieval capacity defines the capacity with respect to the retrieved message *m'*. First of all, zero-bit watermarking schemes do not transmit any message, since the watermark *w* is just detected but a message *m'* is not retrieved. In such a case, the retrieval capacity of these schemes is *zero*.

For non zero-bit watermarking schemes the retrieval capacity is considered *after* data extraction. The following retrieval capacity function is defined: $\text{cap}_{R\text{rel}}(\Omega^*, S_{EA}) = |m| - \sum_{i=1}^{|m|} m_i \oplus m'_i$, where $m = m_1 m_2 \dots m_{|m|}$, $m' = m'_1 m'_2 \dots m'_{|m|}$ and $\oplus$ depicts the exclusive or operation. This equation counts the number of correctly transmitted bits (those which are equal on both sides of the communication channel) and it is assumed that *m* and *m'* have exactly the same length (otherwise *m* or *m'* should be padded or cut in some manner).

In case of repeat coding, the retrieved message is several times longer than the embedded message: $m' = m'_{11} m'_{12} \dots m'_{1|m|} m'_{21} m'_{22} \dots m'_{2|m|} \dots\dots m'_{p_{\max}|m|}$. In such a situation, the retrieval capacity should consider all the repetitions as follows where $p_{\max}$ is the counted number of maximal retrieved *m'*. In the sequel, no repeat

consider all the repetitions as follows $\mathrm{cap}^*_{R\mathrm{rel}}(\Omega^*, S_{EA}) = \sum_{j=1}^{p_{\max}} \left[|m| - \sum_{i=1}^{|m|} m_i \oplus m'_{ji} \right]$,where $p_{\max}$ is the counted number of maximal retrieved m'. In the sequel, no repeat coding is assumed for notational simplicity, but all the formulae can be easily extended to that case. If the watermark is not embedded multiple times, then $p_{\max} = 1$.

There are two relevant comments about this definition of relative capacity. The first is that usually this kind of measure is given in terms of the size of the cover object S: and it is assumed that the sizes of S, and S_{EA} are, at least, similar. This second definition provides measures such as bits per second or in bits of transmitted information per bit of the marked object. If the latter is used, a value in the interval [0,1] is obtained, where 1 means that all the transmitted bits are used for the message, which is the best case as capacity is concerned. The second comment is that is relative to a given pair S_{EA} and S. An absolute measure is provided below.

Another capacity measure can be defined in terms of the ratio of correctly recovered bits normalized by $p_{\max}$. If $p_{\max}$ is unknown, the measure of $\mathrm{cap}^{\$}_{R\mathrm{rel}}$can also be used, but would result in highest, not normalized values.:

$$\mathrm{cap}^{\$}_{R\mathrm{rel}}(\Omega^*, S_{EA}) = \frac{\mathrm{cap}^*_{R\mathrm{rel}}(\Omega^*, S_{EA})}{|m| p_{\max}}.$$

Complexity

Given a function F, the complexity of it can be measured. Thereby the effort or investment needed to embed or attack or detect and retrieve the watermark is defined with complexity. A measuring function C is defined as $C(F)$ to measure the complexity of F. If it is adapted to, for example, the embedding function of Ω, then the embedding complexity can be computed $C(E,S)$. Depending on C, for example the computation cost of time, needed memory or IO operations, lines of code, etc. could be measured. The relative complexity of a watermarking scheme Ω^* and a particular object S is defines as: $C(E,S) \rightarrow \mathrm{com}^*_{\mathrm{rel}}(\Omega^*, S)$However, this definition of complexity depends on the signal S. Thereby, a normalization is needed to provide results independent on S. The normalization can be done with the signal and it length (or size) or with the embedded capacity. If the length (or size) of the signal is used for normalization, then the length can be time or size needed for streaming or file size on the storage. Which exactly is defined with the function size(S). The normalization done by the embedding capacity measures the needed effort to embed one single bit. Note, that this normalization is only usable for n-bit watermarking schemes. In the following both normalizations are formalized.

$$\mathrm{com}^S_{\mathrm{rel}}(\Omega^*, S) = \frac{\mathrm{com}^*_{\mathrm{rel}}}{\mathrm{size}(S)} = \frac{C(E,S)}{\mathrm{size}(S)}$$Note, that in this case a linear complexity depending on the length of S is assumed. If it is non-linear, then this function cannot be used to measure the complexity. Then, the normalization depending on, for example, the embedding capacity, introduced in the following can be used.

$$\mathrm{com}^C_{\mathrm{rel}}(\Omega^*, S) = \frac{\mathrm{com}^*_{\mathrm{rel}}}{\mathrm{cap}^*_E} = \frac{C(E,S)}{\mathrm{cap}^*_E}$$Both definitions of complexity are related to a particular object S. Similar to other watermark properties, a definition of absolute values applies any of the following definitions:

- Average complexity based on signal and capacity normalization: $\mathrm{com}^S_{\mathrm{av}}(\Omega^*) = \frac{1}{|\mathbb{S}|} \sum_{S \in \mathbb{S}} \mathrm{com}^S_{\mathrm{rel}}(\Omega^*, S)$

  $\mathrm{com}^C_{\mathrm{av}}(\Omega^*) = \frac{1}{|\mathbb{S}|} \sum_{S \in \mathbb{S}} \mathrm{com}^C_{\mathrm{rel}}(\Omega^*, S)$
- Maximum complexity for audio signal and capacity normalization: $\mathrm{com}^S_{\mathrm{mx}}(\Omega^*) = \max_{S \in \mathbb{S}} \{\mathrm{com}^S_{\mathrm{rel}}(\Omega^*, S)\}$

  $\mathrm{com}^C_{\mathrm{mx}}(\Omega^*) = \max_{S \in \mathbb{S}} \{\mathrm{com}^C_{\mathrm{rel}}(\Omega^*, S)\}$

- Minimum complexity for audio signal and capacity normalization: $\mathrm{com}^{S}_{\mathrm{inn}}(\Omega^*) = \min_{S \in \mathbb{S}} \{\mathrm{com}^{S}_{\mathrm{rel}}(\Omega^*, S)\}$ $\mathrm{com}^{C}_{\mathrm{inn}}(\Omega^*) = \min_{S \in \mathbb{S}} \{\mathrm{com}^{C}_{\mathrm{rel}}(\Omega^*, S)\}$

Invertibility

Refers to the property of a watermarking scheme which has the possibility to remove the watermark *w* from the marked signal S_E completely to receive signal S' and if Ω is invertible, then $S = S'$. To provide this feature, the watermarking algorithms must provide special embedding techniques. Furthermore, secret keys are mostly used to protect the original content from unauthorized access. The measured value of invertibility for a watermarking scheme Ω^* is a boolean value. If this value is 0, then Ω^* cannot remove *w* from the marked object. If Ω can remove *w* completely and $S = S'$, then 1 is returned.

Robustness

In this section, the robustness of a digital watermarking scheme is described. To introduce the robustness itself, the *detection success* is needed and introduced as first.

Detection Success

To measure the overall success of a detection or retrieval function, the *detection success* function is introduced. Therefore, the connection to zero-bit an n-bit watermarking scheme are introduced as follows. For zero-bit watermarking schemes, $\det_D$D returns 0, if the watermark could not be successful detected and 1 if the detection function was able to detect the watermark, see the following equation: $\det_D(\Omega^*, S_{EA}) = \begin{cases} 0, \text{no successful detection (negative)}, \\ 1, \text{positive successful detection (positive)}. \end{cases}$ To measure the successfully embedding rate over a test set $\mathbb{S}$, the average of $\det_D$ can be computed as follows: $\det_{D\mathrm{av}}(\Omega^*) = \frac{1}{|\mathbb{S}|} \sum_{S \in \mathbb{S}} \det_D$For n-bit watermarking schemes, it is important to know, if the watermark was successfully detected at least once (in case of multiple embedding). If, for example, a watermark scheme embeds the message *m* multiple times $(p_{\max})$, and the retrieval function $\mathrm{cap}^{*}_{R\mathrm{rel}}$returns, that 10% are positive retrievable, then it is unknown, which m_i are affected. Therefore, it is useful to define a successful detection, if at least one embedded message could be retrieved positively, which is introduced in the following equation.

$$\det_R(\Omega^*, S_{EA}) = \begin{cases} 1, \exists j \in \{1, \ldots, p_{\max}\} : \sum_{i=1}^{|m|} m'_{ji} \oplus m_{ji} = 0. \\ 0, \text{otherwise.} \end{cases}$$ Note that this is not the only possible definition of the detection function in case of repeat coding. For example, another definition could be the following:

$$\det_{R\tau}(\Omega^*, S_{EA}) = \begin{cases} 1, \text{if } \mathrm{cap}^{\$}_{R\mathrm{rel}}(\Omega^*, \tilde{S}) \geq \tau. \\ 0, \text{otherwise.} \end{cases}$$ i.e. detection is reported if the ratio of correctly recovered bits is above some threshold τ (which is equal to or close to 1).

Watermark Robustness

The robustness measure $\mathrm{rob}_{\mathrm{rel}}$ of a watermarking scheme is a value in the closed interval [0,1], where 0 is the worst possible value (the scheme is not robust for the signal S) and 1 is the best possible value (the method is robust for the signal S). There is a difference, for example, depending on whether the bit error rate (BER) or byte error rate (BYR) is

used to measure the robustness. If the robustness is measured based on the byte error rate rob^{byte}, then a given watermarking scheme is classified as robust if the bytes of the embedded massage (characters) are correctly retrieved. This measurement is similar to the Levenstein distance, which works and measured a distance between two given strings. It is useful in applications scenarios that need to determine how similar two strings are. Another robustness measure function based on the bit error rate rob^{bit} returns the percentage robustness of the watermarking scheme measured over the whole attacking and test set and is based on the bit changes within the retrieved message. This measurement is similar to the Hamming distance based on bit-strings. Hence, a watermarking scheme is classified as not robust, if more than ν numbers of retrieved bits are destroyed and the transparency of the attacks if higher than τ. For zero-bit watermarking schemes no retrieval function exists and no classification based on bit or byte error rates are possible. To simplify matters, the robustness measure for zero-bit watermarking schemes is always classified to rob^{byte}.

The following example motivates the distinction between the robustness measure based on bit and byte error rate. If the message m="123", with 3 bytes and 3*8=24 bits, is embedded and after attacking, the last 6 bits are destroyed and incorrectly retrieved, then the byte error rate returns, that 2 bytes are correct (the first two) and one is false (the last), which has a value of $\frac{1}{3} = 0.3\overline{3}$. The bit error rate returns, that 18~bits are correct (the first) and 6 bits are false (the last), which has a value of $\frac{6}{24} = 0.25$. If now the 1., 2., 8., 9., 16. and 17. bit are destroyed, then the byte error rate returns, that all bytes (characters) are false and the result has a value of $\frac{3}{3} = 1.0$ and this shows, that 100% of the bytes are destroyed. In contrast, the bit error rate returns, that 18 bits are correct retrieved and 6 bits are wrong, which has a value of $\frac{6}{24} = 0.25$. Although the bit error rate does not change to the first example, differences are apparent in the byte error rater. Therefore, the following equations introduce the robustness for n-bit watermarking schemes divided into rob^{byte} and rob^{bit} and for zero-bit watermarking schemes only for rob^{byte}. The two robustness measures rob^{byte} and rob^{bit} returns completely different robustness values. It is introduced to show, that different approaches are possible and depending on test goals, choices are to be made to select the measure function. It is noted, that different measure methods are available to measure the robustness, i.e. based on det_R in relation to attacking transparency.

The following function relates robustness based on the byte error rate to transparency for a zero-bit and n-bit watermarking scheme as follows, given $S_{EA} = A_{i,j}(S_E)$:

$$\text{rob}_{\text{rel}}^{byte}(\Omega^*, S_E) = 1 - \max_{A_{i,j} \in \mathcal{A}} \left\{ T(S_E, S_{EA}) : \text{det}_D\left(S_{EA}, p_E^{\text{opt}}, p_D^{\text{opt}}, p_{\text{cod}}, [S, m]\right) = 0 \right\}$$

and for a n-bit watermarking scheme:

$$\text{rob}_{\text{rel}}^{byte}(\Omega^*, S_E) = 1 - \max_{A_{i,j} \in \mathcal{A}} \left\{ T(S_E, S_{EA}) : \text{det}_R\left(S_{EA}, p_E^{\text{opt}}, p_D^{\text{opt}}, p_{\text{cod}}, [S, m]\right) = 0 \right\}$$

And the robustness based on the bit error rate related to the transparency for n-bit watermarking schemes is given as:

$$\text{rob}_{\text{av}}^{bit}(\Omega^*) = \frac{1}{|S_{EA}||\mathbb{A}|} \sum_{S \in \mathbb{S}} \sum_{A_{i,j} \in \mathbf{A}} \begin{cases} 1, & (\text{cap}_{R\text{rel}}^{\$} < \tau) \wedge (\text{tra}_{A\text{rel}} > \nu) \\ 0, & \text{otherwise} \end{cases}$$

That is, given a marked object S_E and all the attacks which attack the watermark, even for optimal embedding and detection parameters ($p_E^{\text{opt}}, p_D^{\text{opt}}$), the one which produces less distortion in the marked object S_E determines how robust the scheme is. If none of the attacks in the family $\mathbf{A}$erases the embedded mark, then this measure is (by definition) equal to 1 (the best possible value).

The functions measure robustness in a worst case sense. When the security of a system is to be assessed, it is usually considered that a given system is as weak as the weakest of its components. Similarly, the equation establishes that the worst possible attack (in the sense that the mark is erased but the attacked signal preserves good quality) in a given family

determines how robust the watermarking scheme Ω is. If the best (maximum) transparency amongst all the attacks which destroy the mark is 0.23, then the robustness of the method as given by is $1 - 0.23 = 0.77$.

However, the functions of the equation introduced above are \textit{relative} to a given object S_{EA} (hence the use of the subindex "rel") but usually to define the robustness of a watermarking scheme as an inherent property not related to any particular object, but to a family or collection of objects. This may be referred to as the absolute robustness () which can be defined in several ways. Given a family of cover objects, and their corresponding marked objects S_E obtained by means of the embedding, the absolute robustness based on bit and byte error rate can be defined according to different criteria, for example:

- Average robustness based on byte error rate: * Minimum robustness (worst case approach) based on byte error rate:
- Probabilistic approach based on byte error rate: where *p* stands for ``probability *and r is some given threshold. For example, if r = 0.75 and* $rob_{prob} = 0.9$*, this means that 90% of the objects in* $\mathbb{S}$ *provide a relative robustness greater than or equal to 0.75 for the scheme Ω. Although a maximum robustness measure could thus be defined, it does not seem to have any applicability, since worst or average cases are often reported as robustness is concerned.*

Security

Described the security of the embedded watermark against specific security attacks. After defining all required security measurements $\mathcal{L}$ (like collusion or subspace security), the relative total security $\mathbf{sec}_{\mathbf{rel}}^{\mathbf{tot}}$ can be computed for a particular cover signal. $\mathbf{sec}_{\mathbf{rel}}^{\mathbf{tot}}(\Omega^*, S) = \frac{1}{|\mathcal{L}|} \sum_{\mathbf{sec}_{\mathbf{rel}}^* \in \mathcal{L}} \mathbf{sec}_{\mathbf{rel}}^*(\Omega^*, S)$ Whereby $\mathbf{sec}_{\mathbf{rel}}^*$ defines each relative security measurement provided by $\mathcal{L}$, for example, subspace security $\mathbf{sec}_{\mathbf{rel}}^{\mathbf{sub}}$ or collusion security $\mathbf{sec}_{\mathbf{rel}}^{\mathbf{col}}$ and all other security measurements defined in the security set $\mathcal{L}$. If the average total security $\mathbf{sec}_{\mathbf{av}}^{\mathbf{tot}}$, maximum $\mathbf{sec}_{\mathbf{mx}}^{\mathbf{tot}}$ and minimum $\mathbf{sec}_{\mathbf{mn}}^{\mathbf{tot}}$ are measured, then the following definition are used.

- Average total security: $\mathbf{sec}_{\mathbf{av}}^{\mathbf{tot}}(\Omega^*) = \frac{1}{|\mathbb{S}||\mathcal{L}|} \sum_{S \in \mathbb{S}} \sum_{\mathbf{sec}_{\mathbf{av}}^* \in \mathcal{L}} \mathbf{sec}_{\mathbf{av}}^*(\Omega^*, S)$
- Maximum total security: $\mathbf{sec}_{\mathbf{mx}}^{\mathbf{tot}}(\Omega^*) = \max_{S \in \mathbb{S}} \left\{ \max_{\mathbf{sec}_{\mathbf{mx}}^*} \{\mathbf{sec}_{\mathbf{rel}}^*(\Omega^*, S)\} \right\}$
- Minimum total security: $\mathbf{sec}_{\mathbf{mn}}^{\mathbf{tot}}(\Omega^*) = \min_{S \in \mathbb{S}} \left\{ \min_{\mathbf{sec}_{\mathbf{mn}}^*} \{\mathbf{sec}_{\mathbf{rel}}^*(\Omega^*, S)\} \right\}$

Transparency

Given a reference object S_{ref} and a test object S_{test} the transparency function T provides a measure of the perceptible distortion between S_{ref} and S_{test}. Without loss of generality, such a function may take values in the closed interval [0,1] where 0 provides the worst case (the signals S_{ref} and S_{test} are so different that S_{test} cannot be recognized as a version of S_{ref}) and 1 is the best case (an observer does not perceive any significant difference between S_{ref} and S_{test}):

$$T(S_{\mathbf{ref}}, S_{\mathbf{test}}) \rightarrow [0, 1]$$

The relative transparency for a watermarking scheme Ω^* and a particular object S is defined as:

$$T(S_{\mathbf{ref}}, S_{\mathbf{test}}) \rightarrow \mathbf{tra}_{\mathbf{rel}}(\Omega^*, S)$$

This definition of transparency is related to a particular object *S*. It is usually better to provide some absolute value of

transparency which is not related to a particular object *S*. A definition of "absolute" transparency is related to a family *mathbbS* of objects to be marked, which applies any of the following definitions: * Average transparency:

- Maximum transparency:

- Minimum transparency:

$$\mathrm{tra}_{\mathrm{min}}(\Omega^*) = \min_{S \in \mathbb{S}} \{\mathrm{tra}_{\mathrm{rel}}(\Omega^*, S)\}.$$

Verification

Described the type of the detection/retrieval function *D*,*R* which requires information. Therefore three classifications are available:

Non-blind: If the watermarking scheme requires the cover object *S*, then it is associated as non-blind watermarking scheme. Often, this type of watermark scheme is referred as *informed* watermarking scheme. Mostly, the watermark detector/retriever is only usable from a defined group of people, which hides the watermark detector and the required original signal *S*.

Informed: If the watermarking scheme requires the embedded message *m*, the embedding parameters p_E or other additional information (except the original signal *S*) for detection or retrieval, then the watermarking scheme is associated to this group. Often, watermarking schemes where the embedding function creates a data file needed for detection/retrieval, are associated to this type of verification.

Blind: If the watermarking scheme does not require the original signal nor additional information (e.g. *m* or p_E), then the watermarking scheme is associated to this group. The verification (ver) is defined as list {0,0.5,1}, whereby the 1 is associated with *non-blind*, a 0.5 with *informed* and a 0 with *blind*. The formalization is introduced in the following equation.

$$\mathrm{ver}(\Omega^*, S) = \begin{cases} 0 & (\Omega^*, S) \text{ is non-blind} \\ 0.5 & (\Omega^*, S) \text{ is informed} \\ 1 & (\Omega^*, S) \text{ is blind} \end{cases}$$

Classification

A digital watermark is called **robust** with respect to a class of transformations T if the embedded information can reliably be detected from the marked signal even if degraded by any transformation in T. Typical image degradations are JPEG compression, rotation, cropping, additive noise and quantization. For video content temporal modifications and MPEG compression are often added to this list. A watermark is called **imperceptible** if the cover signal and marked signal are indistinguishable with respect to an appropriate perceptual metric. In general it is easy to create robust watermarks *or* imperceptible watermarks, but the creation of robust **and** imperceptible watermarks has proven to be quite challenging [1]. Robust imperceptible watermarks have been proposed as tool for the protection of digital content, for example as an embedded 'no-copy-allowed' flag in professional video content [2].

Digital watermarking techniques can be classified in several ways.

Robustness

A watermark is called **fragile** if it fails to be detected after the slightest modification. Fragile watermarks are commonly used for tamper detection (integrity proof). Modification to an original work that are clearly noticeable are commonly not referred to as watermarks, but referred to as generalized barcodes.

A watermark is called **semi-fragile** if it resist benign transformations but fails detection after malignant transformations. Semi-fragile watermarks are commonly used to detect malignant transformations.

A watermark is called **robust** if it resists a designated class of transformations. Robust watermarks are commonly used in copyright applications (to carry ownership or forensic information) and copy protection applications (to carry copy and access control information).

Perceptibility

A watermark is called **imperceptible** if the original cover signal and the marked signal are (close to) perceptually indistinguishable.

A watermark is called **perceptible** if its presence in the marked signal is noticeable, but non-intrusive.

Capacity

The length of the embedded message | *m* | determines two different main classes of watermarking schemes:

- | *m* | = 0: The message *m* is conceptually zero-bit long and the system is designed in order to detect the presence or the absence of the watermark *w* in the marked object S_E. This kind of watermarking schemes is usually referred to as *Italic zero-bit* or *Italic presence watermarking schemes*. Sometimes, this type of watermarking scheme is called 1-bit watermark, because a 1 denotes the presence and a 0the absence of a watermark.
- | *m* | = *n* > 0: The message *m* is a n-bit long stream ($m = m_1 \ldots m_n,\ n \in \mathbb{N}$, with *n* = | *m* |) or $M = \{0,1\}^n$ and is modulated in *w*. This kind of schemes is usually referred to as multiple bit watermarking or non zero-bit watermarking schemes.

Embedding method

A watermarking method is referred to as **spread-spectrum** if the marked signal is obtained by an additive modification. Spread-spectrum watermarks are known to be modestly robust, but also to have a low information capacity due to host interference.

A watermarking method is referred to be of **quantization type** if the marked signal is obtained by quantization. Quantization watermarks suffer from low robustness, but have a high information capacity due to rejection of host interference.

A watermarking method is referred to as **amplitude modulation** if the marked signal is embedded by additive modification method which it similar to spread spectrum method but this method is especially embedded in spatial domain.

Applications

Digital Watermarking can be used for a wide range of applications such as:

- Copyright protection.
- Fingerprinting (Different recipients get differently watermarked content).
- Broadcast Monitoring (Television news often contains watermarked video from international agencies).

- Covert Communication (steganography).

Evaluation / Benchmarking

The evaluation of digital watermarking schemes can provide detailed information for watermark designer or end users. Therefore, different evaluation strategies exists. Often used from watermark designer is the evaluation of single properties to show, for example, an improvement. End users, are mostly not interested in detailed information. They want to know, if a given digital watermarking algorithm can be used for their application scenario, and if yes, which parameter sets seems to be the best.

See also

- Copy attack
- Watermark (data file)

External links

- Digital Watermarking Alliance – Furthering the Adoption of Digital Watermarking (http://www.digitalwatermarkingalliance.org/)
- Digital Watermarking & Data Hiding research papers (http://www.forensics.nl/digital-watermarking) at Forensics.nl
- StirMark for Images (http://www.cl.cam.ac.uk/~mgk25/stirmark.html) – Watermarking robustness test developed by Markus Kuhn and Fabien Petitcolas.
- StirMark for Audio (http://wwwiti.cs.uni-magdeburg.de/~alang/smba.php#smba_LA) – Watermarking robustness and fragility test developed by Andreas Lang.
- Directory of Books, Journals & Conferences on Digital Watermarking and Digital Watermarking Assessment Tools (http://knowledgebase.aegisdrm.com/knowledgebase_digital_watermarking_drm.htm)
- Slashdot article (http://slashdot.org/articles/04/11/13/0036243.shtml) – "Warezed SoundForge Files In Windows Media Player"
- Information hiding homepage (http://www.petitcolas.net/fabien/steganography/) by Fabien Petitcolas * Comparison of watermarking methods (http://watermarker.com/how-to-ptotect-digital-images.aspx)
- Watermarking used in monitoring television broadcasts (http://www.business-sites.philips.com/contentidentification/about/Index.html)
- Robust Mesh Watermarking (http://www.cs.princeton.edu/gfx/proj/meshwm/)
- PhotoWaterMark technology: Holographic approach (http://www.smirnov.sp.ru/watermark/cards/card_eng.html)

References

1. ^ I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich and T. Kalker, "Digital Watermarking and Steganography" (Second Edition), Morgan Kaufmann, 2008
2. ^ Copy Protection Technical Working Group (CPTWG) (http://www.cptwg.org/)

- ECRYPT report: Audio Benchmarking Tools and Steganalysis (http://omen.cs.uni-magdeburg.de/ecrypt/deliverables/D.WVL.10-1.1.pdf)
- ECRYPT report: Watermarking Benchmarking (http://omen.cs.uni-magdeburg.de/ecrypt/deliverables/DWVL16_final.pdf)
- Jana Dittmann, David Megias, Andreas Lang, Jordi Herrera-Joancomarti; *Theoretical framework for a practical evaluation and comparison of audio watermarking schemes in the triangle of robustness, transparency and capacity*; In: Transaction on Data Hiding and Multimedia Security I; Springer LNCS 4300; Editor Yun Q. Shi; pp. 1-40; ISBN 978-3-540-49071-5,2006 PDF (http://wwwiti.cs.uni-magdeburg.de/~alang/paper/dittmann_magias_lang_joan-eval_audio_WM_triangle-journal.pdf)
- M. V. Smirnov. Holographic approach to embedding hidden watermarks in a photographic image //Journal of

Optical Technology, Vol. 72, Issue 6, pp. 464-468 (http://jot.osa.org/abstract.cfm?id=85832)

Retrieved from "http://en.wikipedia.org/wiki/Digital_watermarking"
Categories: Authentication methods | Watermarking | Digital photography
Hidden categories: All articles to be merged | Articles to be merged since January 2008

LRB-0686/1
RPN:nok:pg

2007 ASSEMBLY BILL 14

January 12, 2007 – Introduced by Representative SCHNEIDER. Referred to Committee on Judiciary and Ethics.

AN ACT ***to renumber*** 910.01 (1) and 910.01 (4); ***to renumber and amend*** 910.01 (2); ***to amend*** subchapter III (title) of chapter 946 [precedes 946.31]; and ***to create*** 910.01 (1g), 910.025 and 946.33 of the statutes; **relating to:** admissibility of a digitally produced photograph, film, motion picture, audio, or video and providing a penalty.

Analysis by the Legislative Reference Bureau

Under current law, if properly authenticated as being a true representation of the image in the photograph or motion picture, an original of a photograph or motion picture may be admitted in evidence to prove the content of the photograph or motion picture. This bill allows the introduction of a digital representation of a photograph, film, motion picture, audio, or video for purposes of proving the content of that digital representation only if that content has not been altered and is in a format that includes bits representing a watermark scattered within the file in such a way that they cannot be identified or manipulated and that shows that the digital representation has not been altered from its original representation. Digital representation, as defined in the bill, means any recording or image of a person, place, document, sound, or event that is created or stored by data in the form of numerical digits.

The bill creates a misdemeanor for requesting the admission into evidence of a digital representation to prove the contents of that representation if the person knew those contents had been altered.

Because this bill creates a new crime or revises a penalty for an existing crime, the Joint Review Committee on Criminal Penalties may be requested to prepare a report concerning the proposed penalty and the costs or savings that are likely to result if the bill is enacted.

For further information see the ***state and local*** fiscal estimate, which will be printed as an appendix to this bill.

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

SECTION 1. 910.01 (1) of the statutes is renumbered 910.01 (5m).

SECTION 2. 910.01 (1g) of the statutes is created to read:

910.01 **(1g)** DIGITAL REPRESENTATION. "Digital representation" means any recording or image of a person, place, document, sound, or event that is created or stored by data in the form of numerical digits.

SECTION 3. 910.01 (2) of the statutes is renumbered 910.01 (4m) and amended to read:

910.01 **(4m)** PHOTOGRAPHS. "Photographs" include still photographs, X–ray films, ~~and~~ motion pictures, and digital representations.

SECTION 4. 910.01 (4) of the statutes is renumbered 910.01 (2m).

SECTION 5. 910.025 of the statutes is created to read:

910.025 Admissibility of a digital representation. In any action, a digital representation in the form of a photograph, film, motion picture, audio, or video is admissible for purposes of proving the content of that digital representation only if that content has not been altered and is in a format that includes bits representing a watermark that are scattered throughout the file in such a way that they cannot be identified or manipulated and that shows that the digital representation has not been altered from its original representation.

SECTION 6. Subchapter III (title) of chapter 946 [precedes 946.31] of the statutes is amended to read:

CHAPTER 946

SUBCHAPTER III

PERJURY, DIGITAL ALTERATION,

AND FALSE SWEARING

SECTION 7. 946.33 of the statutes is created to read:

946.33 Alteration of a digital representation. (1) In this section, "digital representation" means any recording or image of a person, place, document, sound, or event that is created or stored by data in the form of numerical digits.

(2) Whoever offers into evidence a digital representation for the purpose of proving the content of that digital representation knowing that the digital representation has been altered from its original representation is guilty of a Class A misdemeanor.

SECTION 8. Initial applicability.

(1) This act first applies to actions commenced on the effective date of this subsection.

(END)

D-Note

DRAFTER'S NOTE
FROM THE
LEGISLATIVE REFERENCE BUREAU

LRB-0761/1dn
PJH:...kjf

Date

Representative Schneider,

Enclosed please find a redraft of 2007 AB 14, which limits the admissibility into evidence of certain digital images and audio files. In redrafting this request, I thought of a few issues that may be relevant.

I have done some research on the matter, but it is unclear to me whether digital files are created with watermarks embedded in them or if watermarks are added after the fact. If they are added after the fact, would that constitute an "alteration" of the content of the file? If they are created at the time the digital file is created, do all technologies capable of creating a digital file (e.g., cell phones that are equipped with cameras, digital telephone answering machines) embed watermarks automatically so that images captured by these technologies would be admissible in court? If I take a photograph with my cell phone of a crime in progress, it appears that the photograph would not be admissible in court unless it contains the required watermarks.

Further, what if the fact that a person has altered an image is part of the case? For example, if a person is charged with identify theft, he or she may have altered a photograph on an identification card. Under the wording of this draft, the altered identification card may not be admissible in court.

Please let me know if you would like to discuss this further.

Peggy Hurley
Legislative Attorney
Phone: (608) 266–8906
E–mail: peggy.hurley@legis.wisconsin.gov

DRAFTER'S NOTE
FROM THE
LEGISLATIVE REFERENCE BUREAU

LRB-0761/1dn
PJH:kjf:rs

December 1, 2008

Representative Schneider,

Enclosed please find a redraft of 2007 AB 14, which limits the admissibility into evidence of certain digital images and audio files. In redrafting this request, I thought of a few issues that may be relevant.

I have done some research on the matter, but it is unclear to me whether digital files are created with watermarks embedded in them or if watermarks are added after the fact. If they are added after the fact, would that constitute an "alteration" of the content of the file? If they are created at the time the digital file is created, do all technologies capable of creating a digital file (e.g., cell phones that are equipped with cameras, digital telephone answering machines) embed watermarks automatically so that images captured by these technologies would be admissible in court? If I take a photograph with my cell phone of a crime in progress, it appears that the photograph would not be admissible in court unless it contains the required watermarks.

Further, what if the fact that a person has altered an image is part of the case? For example, if a person is charged with identify theft, he or she may have altered a photograph on an identification card. Under the wording of this draft, the altered identification card may not be admissible in court.

Please let me know if you would like to discuss this further.

Peggy Hurley
Legislative Attorney
Phone: (608) 266-8906
E-mail: peggy.hurley@legis.wisconsin.gov

Duerst, Christina

From: Schneider, Marlin
Sent: Wednesday, February 18, 2009 10:56 PM
To: LRB.Legal
Subject: Draft Review: LRB 09-0761/1 Topic: Admissibility of digitally produced evidence

Please Jacket LRB 09-0761/1 for the ASSEMBLY.

Because this bill creates a new crime or revises a penalty for an existing crime, the Joint Review Committee on Criminal Penalties may be requested to prepare a report concerning the proposed penalty and the costs or savings that are likely to result if the bill is enacted.

For further information see the ***state and local*** fiscal estimate, which will be printed as an appendix to this bill.

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

SECTION 1. 910.01 (1) of the statutes is renumbered 910.01 (5m).

SECTION 2. 910.01 (1g) of the statutes is created to read:

910.01 **(1g)** DIGITAL REPRESENTATION. "Digital representation" means any recording or image of a person, place, document, sound, or event that is created or stored by data in the form of numerical digits.

SECTION 3. 910.01 (2) of the statutes is renumbered 910.01 (4m) and amended to read:

910.01 **(4m)** PHOTOGRAPHS. "Photographs" include still photographs, X-ray films, ~~and~~ motion pictures, and digital representations.

SECTION 4. 910.01 (4) of the statutes is renumbered 910.01 (2m).

SECTION 5. 910.025 of the statutes is created to read:

910.025 Admissibility of a digital representation. In any action, a digital representation in the form of a photograph, film, motion picture, audio, or video is admissible for purposes of proving the content of that digital representation only if that content has not been altered and is in a format that includes bits representing a watermark that are scattered throughout the file in such a way that they cannot be identified or manipulated and that shows that the digital representation has not been altered from its original representation.

SECTION 6. Subchapter III (title) of chapter 946 [precedes 946.31] of the statutes is amended to read:

CHAPTER 946

SUBCHAPTER III

PERJURY, DIGITAL ALTERATION,

AND FALSE SWEARING

SECTION 7. 946.33 of the statutes is created to read:

946.33 Alteration of a digital representation. (1) In this section, "digital representation" means any recording or image of a person, place, document, sound, or event that is created or stored by data in the form of numerical digits.

(2) Whoever offers into evidence a digital representation for the purpose of proving the content of that digital representation knowing that the digital representation has been altered from its original representation is guilty of a Class A misdemeanor.

SECTION 8. Initial applicability.

(1) This act first applies to actions commenced on the effective date of this subsection.

(END)

State of Wisconsin
2009 - 2010 LEGISLATURE

LRB-0761/1
PJH:kjf:rs

2009 BILL

AN ACT ***to renumber*** 910.01 (1) and 910.01 (4); ***to renumber and amend*** 910.01 (2); ***to amend*** subchapter III (title) of chapter 946 [precedes 946.31]; and ***to create*** 910.01 (1g), 910.025 and 946.33 of the statutes; **relating to:** admissibility of a digitally produced photograph, film, motion picture, audio, or video and providing a penalty.

Analysis by the Legislative Reference Bureau

Under current law, if properly authenticated as being a true representation of the image in the photograph or motion picture, an original of a photograph or motion picture may be admitted into evidence to prove the content of the photograph or motion picture. This bill allows the introduction of a digital representation of a photograph, film, motion picture, audio, or video for purposes of proving the content of that digital representation only if that content has not been altered and is in a format that includes bits representing a watermark scattered within the file in such a way that they cannot be identified or manipulated and that shows that the digital representation has not been altered from its original representation. Digital representation, as defined in the bill, means any recording or image of a person, place, document, sound, or event that is created or stored by data in the form of numerical digits.

The bill creates a misdemeanor for requesting the admission into evidence of a digital representation to prove the contents of that representation if the person knew those contents had been altered.

State of Wisconsin
2009 – 2010 LEGISLATURE

LRB-0761/1
PJH:kjf:rs

2009 BILL

AN ACT ***to renumber*** 910.01 (1) and 910.01 (4); ***to renumber and amend*** 910.01 (2); ***to amend*** subchapter III (title) of chapter 946 [precedes 946.31]; and ***to create*** 910.01 (1g), 910.025 and 946.33 of the statutes; **relating to:** admissibility of a digitally produced photograph, film, motion picture, audio, or video and providing a penalty.

Analysis by the Legislative Reference Bureau

Under current law, if properly authenticated as being a true representation of the image in the photograph or motion picture, an original of a photograph or motion picture may be admitted into evidence to prove the content of the photograph or motion picture. This bill allows the introduction of a digital representation of a photograph, film, motion picture, audio, or video for purposes of proving the content of that digital representation only if that content has not been altered and is in a format that includes bits representing a watermark scattered within the file in such a way that they cannot be identified or manipulated and that shows that the digital representation has not been altered from its original representation. Digital representation, as defined in the bill, means any recording or image of a person, place, document, sound, or event that is created or stored by data in the form of numerical digits.

The bill creates a misdemeanor for requesting the admission into evidence of a digital representation to prove the contents of that representation if the person knew those contents had been altered.

Because this bill creates a new crime or revises a penalty for an existing crime, the Joint Review Committee on Criminal Penalties may be requested to prepare a report concerning the proposed penalty and the costs or savings that are likely to result if the bill is enacted.

For further information see the ***state and local*** fiscal estimate, which will be printed as an appendix to this bill.

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

SECTION 1. 910.01 (1) of the statutes is renumbered 910.01 (5m).

SECTION 2. 910.01 (1g) of the statutes is created to read:

910.01 **(1g)** DIGITAL REPRESENTATION. "Digital representation" means any recording or image of a person, place, document, sound, or event that is created or stored by data in the form of numerical digits.

SECTION 3. 910.01 (2) of the statutes is renumbered 910.01 (4m) and amended to read:

910.01 **(4m)** PHOTOGRAPHS. "Photographs" include still photographs, X–ray films, ~~and~~ motion pictures, and digital representations.

SECTION 4. 910.01 (4) of the statutes is renumbered 910.01 (2m).

SECTION 5. 910.025 of the statutes is created to read:

910.025 Admissibility of a digital representation. In any action, a digital representation in the form of a photograph, film, motion picture, audio, or video is admissible for purposes of proving the content of that digital representation only if that content has not been altered and is in a format that includes bits representing a watermark that are scattered throughout the file in such a way that they cannot be identified or manipulated and that shows that the digital representation has not been altered from its original representation.

Insert 1

SECTION 6. Subchapter III (title) of chapter 946 [precedes 946.31] of the statutes is amended to read:

CHAPTER 946

SUBCHAPTER III

PERJURY, DIGITAL ALTERATION,

AND FALSE SWEARING

SECTION 7. 946.33 of the statutes is created to read:

946.33 Alteration of a digital representation. (1) In this section, "digital representation" means any recording or image of a person, place, document, sound, or event that is created or stored by data in the form of numerical digits.

(2) Whoever offers into evidence a digital representation for the purpose of proving the content of that digital representation knowing that the digital representation has been altered from its original representation is guilty of a Class A misdemeanor.

SECTION 8. Initial applicability.

(1) This act first applies to actions commenced on the effective date of this subsection.

(END)

Insert 2

D-Note

INSERT 1:

910.025 Admissibility of a digital representation. (1) In any criminal prosecution, a digital representation in the form of a photograph, film, motion picture, audio, or video that was produced or created by, or on behalf of, a law enforcement officer or agency is admissible for purposes of proving the content of that digital representation only if all of the following are true:

(a) The content of the digital representation has not been altered.

(b) The digital representation is in a format that includes bits representing a watermark that are scattered throughout the file in such a way that they cannot be identified or manipulated.

(c) The watermark described in par. (b) shows that the digital representation has not been altered from its original representation.

(2) This section does not apply if the alteration of the digital representation is an element of the crime that is being prosecuted.

INSERT 5.2

(3) Whoever alters a digital representation with the intent to falsify the content of the digital representation for its use in a criminal prosecution is guilty of a Class A misdemeanor.

(4) Subsection (2) does not apply if the alteration of the digital representation is an element of a crime that is being prosecuted and the digital representation is offered into evidence to prove the element.

LRB-0761/2
???dn
PJH:kjf:rs

DRAFTER'S NOTE
FROM THE
LEGISLATIVE REFERENCE BUREAU

Date

Representative Schneider

Please review this draft to ensure that it is consistent with your intent. This draft applies only to digital representations that originated from a law enforcement agent that are used in criminal prosecutions. The draft makes altering a digital representation with the intent to falsify its contents a class A misdemeanor, and makes knowingly offering an altered digital representation a class A misdemeanor.

Please let me know if you would like further changes to the draft, or if you have any questions.

Peggy Hurley
Legislative Attorney
Phone: (608) 266–8906
E–mail: peggy.hurley@legis.wisconsin.gov

DRAFTER'S NOTE
FROM THE
LEGISLATIVE REFERENCE BUREAU

LRB-0761/2dn
PJH:kjf:rs

October 15, 2009

Representative Schneider

Please review this draft to ensure that it is consistent with your intent. This draft applies only to digital representations that originated from a law enforcement agent that are used in criminal prosecutions. The draft makes altering a digital representation with the intent to falsify its contents a Class A misdemeanor, and makes knowingly offering an altered digital representation a Class A misdemeanor.

Please let me know if you would like further changes to the draft, or if you have any questions.

Peggy Hurley
Legislative Attorney
Phone: (608) 266-8906
E-mail: peggy.hurley@legis.wisconsin.gov